Benjamin A. Schwartzman (SBN 02161)
BAILEY & GLASSER LLP
950 West Bannock Street, Suite 940
Boise, ID 83702
Telephone: (208) 342-4411
Facsimile: (208) 342-4455
bschwartzman@baileyglasser.com
(additional counsel listed on signature page)

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

EUGENE DIVISION

KATELIN MALO, individually, and as natural parent and next friend of A.M., a minor, CORRINNA REED, and JOANN KINDRED, individually and on behalf of all others similarly situated, *Plaintiffs,* v. PERFORMANCE HEALTH TECHNOLOGY, LTD., *Defendant.*	**Case No.:** **CLASS ACTION ALLEGATION COMPLAINT** **JURY TRIAL DEMANDED** **Action for Negligence, Negligence Per Se, Breach of Implied Contract, Oregon Unfair Trade Practices Act (Or. Rev. Stat. § 646.608), Unjust Enrichment, and Injunctive/Declaratory Relief**

Plaintiffs Katelin Malo, individually, and as natural parent and next friend of K.J., a minor, Corrinna Reed, and Joann Kindred (collectively, "Plaintiffs"), individually and on behalf of a class of similarly situated persons, bring this Class Action Complaint and allege the following against defendant Performance Health Technology, Ltd. ("PH Tech" or "Defendant"), based upon personal knowledge with respect to Plaintiffs and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. Plaintiffs bring this class action against PH Tech for its failure to properly secure Plaintiffs' and Class Members' personally identifiable information ("PII") and personal health information ("PHI"). The PII and PHI may have included victims' names, dates of birth, Social Security numbers, contact information, health insurance information, email addresses, diagnostic and procedure codes, and claim and billing information.

2. PH Tech failed to comply with industry standards to protect information systems that contain PII and PHI. Plaintiffs seek, among other things, orders requiring PH Tech to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the disclosure (the "Data Breach") in the future.

3. PH Tech uses MOVEit Transfer ("MOVEit") to exchange files and data between servers, systems, and applications. PH Tech claims that, on May 30, 2023, "attackers [gained] access to [Plaintiffs' and Class Members'] personal information stored on a PH TECH server" via a flaw in the MOVEit software. PH Tech did not discover the until June 2, 2023.

4. On June 16, 2023, PH Tech determined that PII and PHI it received from Health Share of Oregon was breached in the attack.

5. But PH Tech did not disclose that its servers were affected until August 2, 2023, when it reported having sent out notification letters to people whose PII and PHI beginning on July 31, 2023. Plaintiffs received such letters, all dated July 27, 2023.

6. MOVEit Transfer's developer previously reported a security vulnerability in the software in 2021. PH Tech could have prevented the recent Data Breach had it implemented adequate vendor screening after that incident, and maintained adequate data security measures and protocols in order to secure and protect Plaintiffs' and Class Members' data.

7. As a vendor providing electronic health record and cloud-based storage services to customers that collect and store PHI, PH Tech knowingly obtains sensitive PII and PHI and has a resulting duty to securely maintain that information in confidence. Plaintiffs and Class Members would not have provided their PII and PHI to PH Tech customers if they had known that PH Tech would not ensure that it used adequate security measures.

8. Plaintiffs seek to remedy these harms individually and on behalf of all other similarly situated individuals whose PII and/or PHI were stolen in the Data Breach. Plaintiffs seek remedies including compensation for time spent responding to the Data Breach and other types of harm, free credit monitoring and identity theft insurance, and injunctive relief including substantial improvements to PH Tech's data security policies and practices.

PARTIES

9. Plaintiff Katelin Malo is a McMinnville resident who is insured by Health Share of Oregon. Ms. Malo received a letter from PH Tech dated July 27, 2023. Ms. Malo is also suing on behalf of her minor son, A.M., who is also insured by Health Share of Oregon. Ms. Malo received a separate letter from PH Tech addressed to her son dated July 27, 2023.

10. Plaintiff Corrinna Reed is a Portland resident who is insured by Health Share of Oregon. Ms. Reed received a letter from PH Tech dated July 27, 2023.

11. Plaintiff Joann Kindred is a Portland resident who is insured by Health Share of Oregon. Ms. Kindred also received a letter from PH Tech dated July 27, 2023.

12. All Plaintiffs' letters from PH Tech reflect reflects that unauthorized parties accessed Plaintiffs' PII and PHI that may have included the following:

- Name
- Social Security number

- Date of Birth
- Address
- Member and plan ID number
- Email address
- Authorization information
- Diagnosis and procedure codes; and
- Claim and billing information.[1]

13. Defendant Performance Health Technology, Ltd. is an Oregon corporation, with its principal place of business in Salem, Oregon.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Oregon, there are more than 100 class members, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

15. This Court has personal jurisdiction over PH Tech because PH Tech maintains its principal place of business in Oregon and conducts substantial business in this District through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District.

16. Venue is proper in this Court and Division pursuant to 28 U.S.C. § 1391(b)(1) and (2) because PH Tech resides in this District, and this District and Division are where a substantial part of the acts, omissions, and events giving rise to Plaintiffs' claims occurred.

[1] Ex. 1, Notice Letter to Corrinna Reed, at 1.

FACTUAL ALLEGATIONS

The Data Breach

17. PH Tech describes itself as a "company that works with health care plans, helping with things like customer service, enrollment, and payment services."[2] PH Tech claims that "make personal connections to [its customers'] members and providers, empathetically and expertly helping to navigate health care systems. We see your members and providers as our members and providers."[3]

18. Due to the nature of the services it provides, PH Tech acquires and electronically stores PII and PHI. PH Tech was therefore required to ensure that PII and PHI were not disclosed or disseminated to unauthorized third parties without Plaintiffs' and Class Members' express written consent.

19. PH Tech claims that it "discovered [an] attack on one of its servers, on June 2, 2023.[4] PH Tech further claims that it determined on June 16, 2023, that PII and PHI it received from Health Share of Oregon was breached in the attack.[5]

20. On August 2, 2023, PH Tech disclosed that the Data Breach resulted in the exposure of 1.7 million Health Share of Oregon patients' PII and PHI.[6] But PH Tech has apparently not reported the incident to the U.S. Department of Health and Human Services

[2] PH Tech Data Breach FAQS, available at https://phtech.com/notification_faq.html (last visited August 7, 2023).

[3] What We Do, available at https://phtech.com/ (last visited August 7, 2023).

[4] *See* Ex. 1, at 1.

[5] *Id.*

[6] Data breach hits Oregon Health Plan contractor, compromising 1.7 million clients' info, available at https://www.oregonlive.com/business/2023/08/data-breach-hits-oregon-health-plan-ccos-compromising-17-million-customers-info.html (last visited August 7, 2023).

Office for Civil Rights, as is required by law.[7] Nor has it reported the incident to the Oregon Department of Justice.[8]

21. PH Tech's disclosures are otherwise deficient. They do not include basic details concerning the Data Breach, including, but not limited to, why PII and PHI were stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the data was encrypted or otherwise protected, and what PH Tech knows about the degree to which the data has been disseminated.

22. PH Tech has not nearly disclosed all the details of the Data Breach and its investigation. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, PH Tech has taken to secure the PII and PHI still in its possession. Plaintiffs seek to determine the scope of the Data Breach and the information involved, obtain relief that redresses the harm to Plaintiffs' and Class Members' interests, and ensure that PH Tech has proper measures in place to prevent similar incidents from occurring in the future.

PH Tech's Security Representations

23. PH Tech is aware that the Health Insurance Portability and Accountability Act ('HIPAA') requires that PH Tech maintain strict privacy practices.[9] To that end, PH Tech claims

[7] Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited August 7, 2023).

[8] Search Data Breaches, available at https://justice.oregon.gov/consumer/DataBreach / (last visited August 7, 2023).

[9] *See, e.g.*, Change to Covered Relationships display in Demographic Manager and Member Search, available at https://help.phtech.com/hc/en-us/articles/115001173044-Change-to-Covered-Relationships-display-in-Demographic-Manager-and-Member-Search-release-08-15-2017- (last visited August 7, 2023).

to "utilize [Secure File Transfer Protocol ("]SFTP[")] to facilitate the secure transfer of data files."[10] MOVEit's developer likewise purports to "use[] a new SFTP server to align with current SFTP standards."[11]

24. Health care providers access Health Share of Oregon systems via through PH Tech's Clinical Integration Manager software ("CIM")."[12] PH Tech claims that if users "click the "Create Account" button" in the current version of CIM, "[t]his will create all of the necessary account info and security for you to start using CIM3."[13]

The Healthcare Sector is a Primary Target for Data Breaches

25. PH Tech was on notice that companies in the healthcare industry are susceptible targets for data breaches.

26. PH Tech was also on notice that the Federal Bureau of Investigation has been concerned about data security in the healthcare industry. On April 8, 2014, the FBI's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance

[10] SFTP Data Transfer, available at https://help.phtech.com/hc/en-us/articles/360018697720-SFTP-Data-Transfer (last visited August 7, 2023).

[11] Where does information on SSH/SFTP service connections for MOVEit Transfer get logged to?, available at https://community.progress.com/s/article/where-does-information-on-ssh-sftp-connections-for-moveit-transfer-get-logged-to (last visited August 7, 2023).

[12] Provider Portal (CIM), available at https://www.healthshareoregon.org/providers/provider-portal (last visited August 7, 2023).

[13] CareOregon CIM Access Instructions, available at https://help.phtech.com/hc/en-us/articles/360011032319-CareOregon-CIM-Access-Instructions (last visited August 7, 2023).

strategies were working when clearly the data states otherwise." The same warning specifically noted that "[t]he FBI has observed malicious actors targeting healthcare-related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or PII."[14]

27. The number of reported North American data breaches increased by over 50 percent in 2021, from 1,080 in 2020[15], to 1,638 in 2021.[16] As a recent report reflects, "[h]ealthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns."[17]

28. At the end of 2018, the healthcare sector ranked second in the number of data breaches among measured sectors, and had the highest rate of exposure for each breach.[18] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore

[14] Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014), FBI Cyber Division Private Industry Notification (available at https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf) (last accessed Mar. 14, 2023).

[15] *See* Verizon 2021 Data Breach Investigations Report, at 97, https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf (last accessed Mar. 14, 2023).

[16] *See* Verizon 2022 Data Breach Investigations Report, at 83 (available at https://www.verizon.com/ business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf) (last accessed Mar. 14, 2023).

[17] *Id.* at 62.

[18] *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center (available at https://www.idtheftcenter.org/2018-data-breaches) (last accessed Mar. 14, 2023).

coverage.[19] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy.[20]

29. Healthcare-related breaches have persisted because criminals see electronic patient data as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the previous 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[21] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[22]

30. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security

---

[19] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) (available at https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/) (last accessed Mar. 14, 2023).

[20] *Id.*

[21] *2019 HIMSS Cybersecurity Survey* (available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf) (last accessed Mar. 14, 2023).

[22] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Apr. 4, 2019 (available at https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks) (last accessed Mar. 14, 2023).

> of patients' health and financial information, but also patient access to care.[23]

31. As a major healthcare services provider, PH Tech knew, or should have known, the importance of safeguarding Plaintiffs' and Class Members' PII and PHI entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on Plaintiffs and Class Members by virtue of a breach. PH Tech failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

PH Tech Stores Plaintiffs' and Class Members' PII and PHI

32. PH Tech obtains and stores a massive amount of PII and PHI. As a condition of engaging in health care services, PH Tech customers require that patients entrust them with highly confidential PII and PHI.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII and PHI, PH Tech assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII and PHI from disclosure.

34. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and rely on PH Tech to keep this information confidential and securely maintained, and to make only authorized disclosures of this information.

PII and PHI are Valuable and Subject to Unauthorized Disclosure

35. PH Tech was aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

---

[23] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals,* Am. Med. Ass'n (Oct. 4, 2019) (available at https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals) (last visited Mar. 14, 2023).

36. PII and PHI are valuable commodities to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[24] Indeed, a robust illegal market exists in which criminals openly post stolen PII and PHI on multiple underground websites, commonly referred to as the "dark web." PHI can sell for as much as $363 on the dark web, according to the Infosec Institute.[25]

37. PHI is particularly valuable because criminals can use it to target victims with frauds and swindles that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

38. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's PHI is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[26]

---

[24] Federal Trade Commission, What To Know About Identity Theft (available at https://consumer.ftc.gov/articles/what-know-about-identity-theft) (last accessed Mar. 14, 2023).

[25] Center for Internet Security, *Data Breaches: In the Healthcare Sector* (available at https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/) (last accessed Mar. 14, 2023).

[26] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, Kaiser Health News (Feb. 7, 2014) (available at https://khn.org/news/rise-of-indentity-theft/) (last accessed Mar. 14, 2023).

39. The ramifications of PH Tech's failure to keep Plaintiffs' and Class Members' PII and PHI secure are long-lasting and severe. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for months or even years thereafter.

40. Further, criminals often trade stolen PII and PHI for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

41. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [27] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[28]

42. PH Tech knew, or should have known, the importance of safeguarding PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiffs and Class Members because of a breach. PH Tech failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

[27] *See* Medical ID Theft Checklist (available at https://www.identityforce.com/blog/medical-id-theft-checklist-2) (last accessed Mar. 14, 2023).

[28] Experian, The Potential Damages and Consequences of Medical Identityy Theft and Healthcare Data Breaches (available at https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf) (last accessed Mar. 14, 2023).

The Data Breach Exposed Plaintiffs and Class Members to Identity Theft and Out-of-Pocket Losses

43. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of their rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

44. Despite all the publicly available knowledge of known and foreseeable consequences of the disclosure of PII and PHI, PH Tech's policies and practices with respect to maintaining the security of Plaintiffs' and Class Members' PII and PHI were reckless, or at the very least, negligent.

45. In virtually all contexts, the expenditure of time has consistently been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiffs and Class Members should be compensated for the time they have expended because of PH Tech's misfeasance.

46. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[29]

47. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer financial loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their PII and PHI;

b. identity theft and fraud resulting from the theft of their PII and PHI;

[29] 2014 LexisNexis True Cost of Fraud Study (available at https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf) (last accessed Mar. 14, 2023).

c. costs associated with the detection and prevention of identity theft;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

g. the continued imminent injury flowing from potential fraud and identify theft posed by their PII and PHI being in the possession of one or more unauthorized third parties.

PH Tech's Lax Security Violates HIPAA

48. PH Tech had a non-delegable duty to ensure that all PHI it collected and stored was secure.

49. PH Tech is bound by HIPAA (*see* 45 C.F.R. § 160.102) and, as a result, is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

50. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

51. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

52. HIPAA requires that PH Tech implement appropriate safeguards for this information.

53. Despite these requirements, PH Tech failed to comply with its duties under HIPAA and its own Privacy Practices. In particular, PH Tech failed to:

a. maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. adequately protect Plaintiffs' and Class Members' PHI;

c. ensure the confidentiality and integrity of electronic PHI created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. ensure compliance with the electronic PHI security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. train all members of its workforce effectively on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their responsibilities and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b)

54. PH Tech failed to comply with its duties under HIPAA despite being aware of the risks associated with unauthorized access to Plaintiffs' and Class Members' PHI.

PH Tech Violated FTC Guidelines

55. The Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, prohibited PH Tech from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' PII is an "unfair practice" in violation of the FTC Act. *See, e.g., Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

56. The FTC has promulgated several guides for businesses that reflect the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[30]

57. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established data security guidelines for businesses.[31] The guidelines reflect that businesses should protect the PII that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

58. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to confidential data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[32]

59. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting

[30] Federal Trade Commission, Start With Security: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last accessed Mar. 14, 2023).

[31] Federal Trade Commission, Protecting Personal Information: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed Mar. 14, 2023).

[32] FTC, *Start With Security*, *supra*.

from these actions further clarify the measures businesses must take to meet their data security obligations.

60. PH Tech failed to properly implement basic data security practices. PH Tech's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

61. PH Tech was at all times fully aware of its obligation to protect Plaintiffs' and Class Members' PII and PHI because of its position as a healthcare provider. PH Tech was also aware of the significant repercussions that would result from its failure to do so.

CLASS ACTION ALLEGATIONS

62. Pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, Plaintiffs seek certification of a Class as defined below:

> All persons in the United States and its territories whose PII and/or PHI was compromised in the Data Breach.

63. Excluded from the Class are PH Tech, any entity in which PH Tech has a controlling interest, and PH Tech's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

64. Plaintiffs reserve the right to modify or amend the definition of the proposed Class as additional information becomes available to Plaintiffs.

65. **Numerosity:** The Class Members are so numerous that individual joinder of all Class Members is impracticable. PH Tech has disclosed that the Data Breach affected approximately 1.7 million individuals. All Class Members' names and addresses are available

from PH Tech's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

66. **Commonality:** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent PH Tech had a duty to protect the PII and PHI of Class Members;

b. Whether PH Tech was negligent in collecting and storing Plaintiffs' and Class Members' PII and PHI;

c. Whether PH Tech had duties not to disclose the PII and PHI of Class Members to unauthorized third parties;

d. Whether PH Tech took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII and PHI;

e. Whether PH Tech failed to adequately safeguard the PII and PHI of Class Members;

f. Whether PH Tech failed to implement and maintain reasonable security policies and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;

g. Whether PH Tech adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

h. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or punitive damages because of PH Tech's wrongful conduct;

i. Whether Plaintiffs and Class Members are entitled to restitution because of PH Tech's wrongful conduct;

j. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm they face because of the Data Breach; and

k. Whether Plaintiffs and Class Members are entitled to identity theft protection for their respective lifetimes.

67. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII and PHI, like that of every other Class Member, was disclosed by PH Tech. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through PH Tech's common misconduct. Plaintiffs are advancing the same claims and legal theories individually and on behalf of all other Class Members, and there are no defenses that are unique to Plaintiffs. Plaintiffs' claims and Class Members' claims arise from the same operative facts and are based on the same legal theories.

68. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against PH Tech to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' counsel are competent and experienced in litigating class actions, including extensive experience in data breach litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

69. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because PH Tech has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate

with respect to the Class as a whole. PH Tech's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on PH Tech's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

70. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like PH Tech. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

71. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because PH Tech would necessarily gain an unconscionable advantage in non-class litigation, since PH Tech would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by Class Members and will establish the right of each Class Member to recover on the causes of action alleged; and

individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

72. The litigation of Plaintiffs' claims is manageable. PH Tech's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with maintenance of this lawsuit as a class action.

73. Adequate notice can be given to Class Members directly using information maintained in PH Tech's records.

74. Unless a class-wide injunction is issued, PH Tech may continue to maintain inadequate security with respect to the PII and PHI of Class Members, PH Tech may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and PH Tech may continue to act unlawfully as set forth in this Complaint.

75. PH Tech has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

COUNT I
NEGLIGENCE
(on behalf of Plaintiffs and the Class)

76. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

77. PH Tech knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. That duty included, among other things, designing, maintaining, and testing PH Tech's security protocols to ensure that Plaintiffs' and Class

Members' PII and PHI in PH Tech's possession was adequately secured and protected, that Plaintiffs' and Class Members' PII and PHI on PH Tech's networks were not accessible to criminals without authorization, and that PH Tech employees tasked with maintaining such information were adequately trained on security measures regarding the security of Plaintiffs' and Class Members' PII and PHI.

78. Plaintiffs and Class Members entrusted their PII and PHI to PH Tech with the understanding that PH Tech would safeguard their information, use their PII and PHI for business purposes only, and not disclose their PII and PHI to unauthorized third parties.

79. PH Tech knew or reasonably should have known that a failure to exercise due care in the collecting, storing, and using Plaintiffs' and Class Members' PII and PHI involved an unreasonable risk of harm to Plaintiffs and Class Members.

80. PH Tech also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII and PHI.

81. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of prior data breaches and disclosures prevalent in today's digital landscape, including the explosion of data breaches involving similarly situated healthcare providers.

82. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. PH Tech knew or should have known of the inherent risks in collecting and storing Plaintiffs' and Class Members' PII and PHI, the critical importance of providing adequate security of that information, the necessity for encrypting PHI stored on PH Tech's systems, and that it had inadequate IT security protocols in place to secure Plaintiffs' and Class Members' PII and PHI.

83. PH Tech's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. PH Tech's misconduct included, but was not limited to, failure to take the steps and opportunities to prevent the Data Breach as set forth herein.

84. Plaintiffs and Class Members had no ability to protect their PII and PHI that was in PH Tech's possession.

85. PH Tech was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

86. PH Tech had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' PII and PHI within its possession was compromised and precisely the type(s) of information that were compromised.

87. PH Tech had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII and PHI.

88. PH Tech systematically failed to provide adequate security for data in its possession.

89. PH Tech, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' PII and PHI within its possession.

90. PH Tech, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' PII and PHI.

91. PH Tech, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the PII and PHI within PH Tech's possession might have been compromised and precisely the type of information compromised.

92. PH Tech's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' PII and PHI to be compromised.

93. But for all of PH Tech's acts of negligence detailed above, including allowing cyber criminals to access its systems containing Plaintiffs' and Class Members' PII and PHI would not have been compromised.

94. Plaintiffs never transmitted their own unencrypted PHI over the internet or any other unsecured source.

95. Following the Data Breach, Plaintiffs' PHI has been seized by unauthorized third parties who are now free to exploit and misuse that PHI without any ability for Plaintiffs to recapture and erase that PHI from further dissemination—Plaintiffs' PHI is forever compromised.

96. But for the Data Breach, Plaintiffs would not have incurred the loss and publication of their PHI and other injuries.

97. There is a close causal connection between PH Tech's failure to implement security measures to protect Plaintiffs' and Class Members' PII and PHI and the harm suffered, or risk of imminent harm suffered by Plaintiffs and Class Members. Plaintiffs' and Class Members' PHI was accessed and compromised as the proximate result of PH Tech's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures and encryption.

98. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, loss of privacy, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

99. As a result of PH Tech's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their PII and PHI, which is still in the possession of third parties, will be used for fraudulent purposes.

100. Plaintiffs seek the award of actual damages on behalf of themselves and the Class.

101. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling PH Tech to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling PH Tech to provide detailed and specific disclosure of what types of PII and PHI have been compromised as a result of the data breach.

COUNT II
NEGLIGENCE PER SE
(on behalf of Plaintiffs and the Class)

102. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

103. Pursuant to HIPAA (42 U.S.C. § 1302d et seq.) and the FTC Act, PH Tech was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' PHI and PII.

104. The Oregon Unlawful Trade Practices Act ("OUTPA"), Or. Rev. Stat. § 646.608(1), *et seq.*, prohibits unfair or deceptive acts or practices in the conduct of any trade or commerce. In addition to HIPAA, OUTPA requires that PH Tech protect PII and PHI from unauthorized access and disclosure.

105. PH Tech violated HIPAA and OUTPA by failing to comply with applicable industry standards. PH Tech's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored, and the exposure of Plaintiffs' and Class Members' sensitive PII and PHI.

106. PH Tech breached its duties by failing to employ industry standard data and cybersecurity measures to ensure its compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

107. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' PII and PHI in compliance with applicable laws would result in an unauthorized third-party gaining access to PH Tech's networks, databases, and computers that stored or contained Plaintiffs' and Class Members' PII and PHI.

108. PH Tech's violations of HIPAA and OUTPA constitute negligence per se.

109. Plaintiffs and Class Members are within the category of persons HIPAA and OUTPA were intended to protect.

110. The harm that occurred as a result of the Data Breach is the type of harm HIPAA and OUTPA were intended to guard against.

111. Plaintiffs' and Class Members' PII and PHI constitute personal property that was stolen due to PH Tech's negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

112. PH Tech's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' unencrypted PII and PHI, and Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of PH Tech's conduct. Plaintiffs and Class Members seek damages and other relief as a result of PH Tech's negligence.

COUNT III
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiffs and the Class)

113. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

114. When Plaintiffs and Class Members provided their PII and PHI to PH Tech, they entered into implied contracts with PH Tech, under which PH Tech agreed to take reasonable steps to protect Plaintiffs' and Class Members' PII and PHI, comply with it statutory and common law duties to protect Plaintiffs' and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

115. PH Tech solicited and invited Plaintiffs and Class Members to provide their PII and PHI as part of PH Tech's provision of healthcare support services. Plaintiffs and Class Members accepted PH Tech's offers and provided their PII and PHI to PH Tech.

116. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that PH Tech's data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' and Class Members' PII and PHI and to timely notify them in the event of a data breach.

117. PH Tech's implied promise to safeguard PII and PHI is evidenced by, *e.g.*, the representations in PH Tech's privacy policies set forth above.

118. Plaintiffs and Class Members would not have provided their PII and PHI to PH Tech had they known that PH Tech would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

119. Plaintiffs and Class Members fully performed their obligations under their implied contracts with PH Tech.

120. PH Tech breached its implied contracts with Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach.

121. The losses and damages Plaintiffs sustained, include, but are not limited to:

a. Theft of their PII and PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling, and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to PH Tech with the mutual understanding that PH Tech would

safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and PHI, which remains in PH Tech's possession and is subject to further breaches so long as PH Tech fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

122. As a direct and proximate result of PH Tech's breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT IV
VIOLATION OF OREGON UNLAWFUL TRADE PRACTICES ACT
(on behalf of Plaintiffs and the Class)

123. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

124. Plaintiffs are authorized to bring this claim pursuant to Or. Rev. Stat. § 646.638(1).

125. Or. Rev. Stat. § 646.608(1), et seq. ("OUTPA"), prohibits "unlawful practice[]s in the course of the person's business, vocation or occupation. . . ." Or. Rev. Stat. § 646.608(1).

126. PH Tech has engaged in the following unfair or deceptive acts or practices in violation of the OUTPA:

a. "Represent[ing] that … services have … characteristics… or qualities that the … services do not have" in violation of Or. Rev. Stat. § 646.608(1)(e);

b. "Represent[ing] that … services are of a particular standard, quality, or grade …if the … services are of another" in violation of Or. Rev. Stat. § 646.608(1)(g); and

c. "Engag[ing] in any other unfair or deceptive conduct in trade or commerce" in violation of Or. Rev. Stat. § 646.608(1)(u).

127. PH Tech's deceptive acts or practices in the conduct of commerce include, but are not limited to:

a. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII and PHI, including by implementing and maintaining reasonable security measures;

d. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII and PHI; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' PII and PHI.

128. PH Tech is engaged in, and its acts and omissions affect, trade and commerce. PH Tech's relevant acts, practices, and omissions complained of in this action were done in the course of PH Tech's business of marketing, offering for sale, and selling goods and services to consumers.

129. PH Tech had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiffs' and Class Members' PII and PHI.

130. PH Tech had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

131. PH Tech also had exclusive knowledge about the length of time that it maintained individuals' PII and PHI after they stopped using services that necessitated the transfer of that PII to PH Tech.

132. PH Tech failed to disclose, and actively concealed, the material information it had regarding its deficient security policies and practices and regarding the security of the sensitive PII and PHI. During the days and weeks following the Data Breach, PH Tech failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

133. PH Tech had a duty to disclose the material information that it had because, inter alia, it had exclusive knowledge of the information, it actively concealed the information, and

because PH Tech was in a fiduciary position by virtue of the fact that it collected and maintained Plaintiffs' and Class Members' PII and PHI.

134. PH Tech's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of its data security and its ability to protect the confidentiality of patients' PII and PHI.

135. Had PH Tech disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, PH Tech would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, PH Tech received, maintained, and compiled Plaintiffs' and Class Members' PII and PHI without disclosing that its data security practices were insufficient to maintain the safety and confidentiality of that information.

136. Accordingly, Plaintiffs and Class Members acted reasonably in relying on PH Tech's misrepresentations and omissions, the truth of which they could not have discovered.

137. PH Tech's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws such as HIPAA.

138. The injuries suffered by Plaintiffs and Class Members greatly outweigh any potential countervailing benefit to consumers or to competition and are not injuries that Plaintiffs and Class Members should have reasonably avoided.

139. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and Class Members as a direct result of PH Tech's deceptive acts and practices as set forth herein include, without limitation:

a. theft of their PII and PHI;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts and PHI;

c. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

d. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

e. damages to and diminution in value of their PII and PHI entrusted to PH Tech, and with the understanding that PH Tech would safeguard their data against theft and not allow access and misuse of their data by others; and

f. the continued risk to their PII and PHI, which remains in the possession of PH Tech, and which is subject to further breaches so long as PH Tech fails to undertake appropriate and adequate measures to protect data in its possession.

140. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring PH Tech from disclosing their PII and PHI without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT V
UNJUST ENRICHMENT
(on behalf of Plaintiffs and the Class)

141. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

142. Plaintiffs and Class Members have an interest, both equitable and legal, in their PHI and PII that was conferred upon, collected by, and maintained by PH Tech and that was stolen in the Data Breach.

143. PH Tech benefitted from the conferral upon it of Plaintiffs' and Class Members' PII and PHI, and by its ability to retain and use that information. PH Tech understood that it so benefitted.

144. PH Tech also understood and appreciated that Plaintiffs' and Class Members' PHI and PII was private and confidential and that its value depended upon PH Tech maintaining its privacy and confidentiality.

145. But for PH Tech's willingness and commitment to maintain its privacy and confidentiality, that PHI and PII would not have been transferred to and entrusted with PH Tech. Further, if PH Tech had disclosed that its data security measures were inadequate, PH Tech would not have been permitted to continue in operation by regulators and the healthcare marketplace.

146. As a result of PH Tech's wrongful conduct as alleged in this Complaint (including, among other things, its failure to employ adequate data security measures, its continued maintenance and use of Plaintiffs' and Class Members' PHI without having adequate data security measures, and its other conduct facilitating the theft of that PHI and PII), PH Tech has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

147. PH Tech's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiffs' and Class

Members' sensitive PHI and PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers.

148. Under the common law doctrine of unjust enrichment, it is inequitable for PH Tech to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiffs' and Class Members' PHI and PII in an unfair and unconscionable manner. PH Tech's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

149. The benefit conferred upon, received, and enjoyed by PH Tech was not conferred officiously or gratuitously, and it would be inequitable and unjust for PH Tech to retain the benefit.

COUNT VI
INJUNCTIVE/DECLARATORY RELIEF
(on behalf of Plaintiffs and the Class)

150. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

151. PH Tech owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure PII and PHI.

152. PH Tech still stores Plaintiffs' and Class Members' PII and PHI.

153. Since the Data Breach, PH Tech has announced no specific changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent similar incidents from occurring in the future.

154. PH Tech has not satisfied its legal duties to Plaintiffs and Class Members.

155. Actual harm has arisen in the wake of the Data Breach regarding PH Tech's duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs

and Class Members are at risk of additional or further harm due to the exposure of their PII and PHI, and PH Tech's failure to address the security failings that led to that exposure.

156. Plaintiff, therefore, seeks a declaration: (a) that PH Tech's existing security measures do not comply with its duties of care to provide adequate security; and (b) that to comply with its duties of care, PH Tech must implement and maintain reasonable security measures, including, but not limited to, the following:

a. ordering that PH Tech engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on PH Tech's systems on a periodic basis, and ordering PH Tech to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that PH Tech engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that PH Tech audit, test, and train its security personnel regarding any new or modified procedures;

d. ordering that PH Tech segment PHI by, among other things, creating firewalls and access controls so that if one area of PH Tech's system is compromised, hackers cannot gain access to other portions of PH Tech's systems;

e. ordering that PH Tech purge, delete, and destroy in a reasonably secure manner PII and PHI not necessary for its provision of services;

f. ordering that PH Tech conduct regular computer system scanning and security checks; and

g. ordering that PH Tech routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, prays for relief as follows:

a. for an Order certifying the Class as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

b. for equitable relief enjoining PH Tech from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

c. for equitable relief compelling PH Tech to use appropriate cyber security methods and policies with respect to PII and PHI collection, storage, and protection, and to disclose with specificity to Class Members the types of PII and PHI compromised;

d. for an award of damages, including actual, nominal, consequential, enhanced compensatory, and punitive damages, as allowed by law in an amount to be determined;

e. for an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. for prejudgment interest on all amounts awarded; and

g. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: August 7, 2023

Respectfully submitted,

BAILEY & GLASSER LLP

/s/ Benjamin A. Schwartzman

Benjamin A. Schwartzman (SBN 02161)
950 West Bannock Street, Suite 940
Boise, ID 83702
Telephone: (208) 342-4411
Facsimile: (208) 342-4455
bschwartzman@baileyglasser.com z

BAILEY GLASSER LLP
John W. Barrett
209 Capitol Street
Charleston, WV 25301
(304) 345-6555
jbarrett@baileyglasser.com

BAILEY GLASSER LLP
Bart D. Cohen
Lawrence J. Lederer
1622 Locust Street
Philadelphia, PA 19103
(215) 274-9420
bcohen@baileyglasser.com
llederer@baileyglasser.com

THE CONSUMER PROTECTION FIRM, PLLC
William "Billy" Peerce Howard
401 East Jackson Street, Suite 2340
Truist Place
Tampa, FL 33602
(813) 500-1500
Billy@TheConsumerProtectionFirm.com

Attorneys for Plaintiffs and the Proposed Class